**IN THE SPECIFICATION**

Please replace the first full paragraph, of page 1 with the following amended paragraph:

This application claims the benefit of U.S. provisional applications 60/138,849, 60/138,850,60/139,033, 60/139,034, 60/139,035, 60/139,036, 60/139,038, 60/139,042, 60/139,043, 60/139,044, 60/139,047, 60/139,048, 60/139,049, 60/139,052, 60/139,053, all filed on June 10, 1999, and U.S. provisional application 60/139,076, filed on June 11, 1999, the contents of all of which are incorporated herein by reference. This application also contains subject matter that is related to the subject matter disclosed in U.S. Patent Application Nos. 09/592,443, 09/591,802, 09/592,165, 09/591,801 now U.S. Patent no. 6,708,187, 09/592,163, 09/592,079, and 09/592,083 now U.S. Patent no. 6,678,835, all filed on June 12, 2002.

Please replace the fourth full paragraph, of page 1 with the following amended paragraph:

In managing the growth of computer networks as well as addressing the various security issues, network managers often turn to network policy management services such as firewall protection, Network Address Translation, spam email filtering, DNS caching, Web caching, virtual private network (VPN) organization and security, and URL blocking for keeping network users from accessing certain ~~Web~~ web sites through the use of the organization's ISP. Each policy management service, however, generally requires a separate device that needs to be configured, managed, and monitored. Furthermore, as an organization grows and spreads across multiple locations, the devices maintained also multiplies, multiplying the associated expenditures and efforts to configure, manage, and monitor the devices.

Please replace the first full paragraph, of page 9 with the following amended paragraph:

As illustrated in FIG. 2, each object in the structure is preferably stored as an LDAP entry. At the top of the hierarchy is the policy server domain object 201 including various policy server resources and a plurality of policy ~~domains~~ domain objects (generally referenced at 204). Each policy domain object 240 is a grouping of policy enforcers that share common policies. Each, policy domain object 240 includes a resource root object 200 and a group root object 202. All policy management functions are preferably implemented in terms of the resource objects, which include devices 204, users 206, hosts 208, services 210, and time 220. Thus, a firewall policy may be defined by simply assigning the particular devices, users, hosts, services, and time applicable to the policy. The devices, users, hosts, and services are preferably organized in groups 212, 214, 216, and 218, respectively, having a group name, description, and member information for a more intuitive way of addressing and organizing the resources.

Please replace the second full paragraph, of page 14 with the following amended paragraph:

Once connected, the policy enforcer installation wizard 406 invokes the interactive user interface to assist the network administrator in setting up a particular policy enforcer 124, 126. Among other things, the policy enforcer installation wizard [[464]] 406 prompts the administrator to specify the policy server IP address, policy enforcer IP address, and router IP address. The policy enforcer then registers with the policy server 122 by invoking a URL on the policy server with basic bootstrap information of its own. The registration of the policy enforcer allows the initialization of the policy enforcer's database 132, 134 with the configuration information, as well as the monitoring of the policy enforcer's status and health by the policy server 122.

Please replace the third full paragraph, of page 17 with the following amended paragraph:

Selection of the devices tab 718b causes a display of various device management icons for managing the policy server 122 and the policy enforcers 124, 126 as is illustrated in FIG. 9. A policy server ~~systems~~ system settings icon 750 allows the network administrator to

view and modify system settings like LAN, WAN/DMS IF addresses of the policy server 122. A policy server archive options icon 752 allows specification of reporting and other database archive options at the policy server 122. A global URL blocking icon 754 allows the administrator to specify a list of unauthorized web sites 116 to be blocked by all the policy enforcers 124, 126 of the system. Similarly, a global spam list icon 756 allows the administrator to specify a list of email addresses of spammers 118 to be blocked by all the policy enforcers

Please replace the fourth full paragraph, of page 20 with the following amended paragraph:

Preferably, the user attribute 734 indicates the user groups and users that are eligible for the policy. The source attribute 736 indicates a point of origination of the network traffic associated with the user. The services attribute 738 indicates the services to [[the]] be allowed or denied by the policy. The destination attribute indicates a specific LAN, WAN, DMS segment or specific hosts where the specified services are to be allowed or denied. For example, to configure SMTP pop services on a mail server, the host may be the IP address where the mail server is running, and the services specified is SMTP. The time attribute indicates a time slot in which the policy is to be effective [[,]] .

Please replace the third full paragraph, of page 21 with the following amended paragraph:

As illustrated in FIG. 14, a new firewall policy may be defined by simply adding a description of the policy in a description area 728a, selecting an action to be applied to the matching network traffic in an action box 730a, and indicating in an active area 732a whether the policy is to be active or inactive. Furthermore, the network administrator specifies the user, source, services, destination, and time resources in a user area 734a, source area 736a, services area 738a, destination area [[739a]] 739, and time area 741, respectively. The network administrator further selects an authentication scheme for the policy in an authentication area 743. Upon actuation of an OK button 745, appropriate entries of the policy server database's LDAP tree are suitably changed to reflect the addition of the new

policy. The change is also transmitted to the respective policy enforcers as is described in further detail below.

Please replace the second full paragraph, of page 27 with the following amended paragraph:

Remote users communicate over the public Internet 108 with the other members of the VPN behind policy enforcers 124, 126, upon presenting appropriate credentials These remote users access the private networks as VPN clients 140 using [[a]] VPN client software. According to one embodiment of the invention, the system allows the remote user to download a self-extracting executable which, upon execution, installs both the VPN client software and VPN reachability information unique to the remote user in the user's remote terminal.

Please replace the third full paragraph, of page 28 with the following amended paragraph:

The self-extracting executable 290 preferably includes an executable setup file 292 for installing the VPN client software and/or the VPN configuration information. The setup file 292 preferably forms a static portion 298 of the self-extracting executable since this information does not change based on the downloading VPN client. The self-extracting executable 290 further includes VPN configuration file templates for the VPN reachability information 294 and the VPN client's preshared key information 296. The VPN reachability information 294 and the VPN client's preshared key 296 preferably form a dynamic portion 299 of the self—extracting executable 290 since this information changes based on the downloading VPN client. The self-extracting executable 290 is then saved as a template file in the policy enforcers 124, 126 and is ready to [[the]] <u>be</u> downloaded by the remote users.

Please replace the first full paragraph, of page 30 with the following amended paragraph:

## VI. ~~INTEGATED~~ INTEGRATED POLICY ENFORCER

According to one embodiment of the invention, the functionalities of the policy enforcer 124, 126 for policy enforcement are partitioned for effective hardware implementation. However, it should be apparent to one skilled in the art that some or all of the functionalities may be implemented in software, hardware, or various combinations thereof.

Please replace the third full paragraph, of page 32 with the following amended paragraph:

A decision engine 606 includes logic to serve the incoming policy decision requests in the policy request table 602 by matching it against the policy rule set in the policy rules database buffer 608 based on the actual membership information obtained from the resource engine 604. The relevant group-based rule matching the traffic is then identified and decision bits in the stream table are set for enforcing the corresponding actions. The decision bits thus constitute the set of actions to be performed on the packets of the stream. All packets matching the streams are then processed based on these decision bits. The decision engine may also specify an access control list (ACL) including a set of rules that allow/deny traffic, a DiffServ standard for providing a quality of service level to the traffic, and/or VPN implementation information.

Please replace the first full paragraph, of page 34 with the following amended paragraph:

FIG. 21 is a more detailed schematic block diagram of the IPSec engine 502 according to one embodiment of the invention. As illustrated in FIG. 21, the IPSec engine 502 includes a Pseudo-Random Number Generator (PRNG) function 802 for generating random numbers used for cryptographic key generation according to well known methods. [[A ]] Diffie Hellman 804 and RSA 812 blocks implement the corresponding asymmetric public key encryption/decryption/signature algorithms which are also well known in the art. An IKE block 806 communicates with an IPSec SA table 808 for implementing standard

ISAKMP/Oakley(IKE) key a packet was received, as well as a destination IP address and port 826 indicating the destination to which the packet was forwarded.

Please replace the second full paragraph, of page 36 with the following amended paragraph:

A person skilled in the art should recognize that additions, deletions, and other types of modifications may be made to the log format without departing from the spirit and the scope of the invention as long as the log format common to all the policy enforcers [[and]] is aimed in creating compact logs.

Please replace the fourth full paragraph, of page 36 with the following amended paragraph:

Once the policy server 122 receives the logs, it is stored in the archive database 318 preferably taking the form of [[an]] a SQL database. The policy server reports module 316 queries this database to generate reports for each policy enforcer 124, 126. In addition, the logs may be exported in a format that may be interpreted by commercially available products such as WEBTRENDS, manufactured by WebTrends Corporation of Portland, Oregon.

Please replace the first full paragraph, of page 39 with the following amended paragraph:

FIG. 24 is a more detailed block diagram of branch 270 of 15 the LDAP tree of FIG. 23. The LDAP root 265 includes an ApplyLog 270a entry which in turn includes a user log entry 270b and a device log entry 270c. The user log entries include specific administrator log entries identified by specific DNs 270d for reflecting the changes made by the particular administrators. The device log entry 270c includes specific device log entries identified by specific DNs 270e reflecting the changes that are to be distributed to the particular policy ~~enforces~~ enforcers 124, 126. Preferably, the changes made by the administrators are propagated to the policy enforcers 124, 126 upon actuation of an apply

button such as the apply button 417 illustrated in FIG. 6.

Please replace the third full paragraph, of page 39 with the following amended paragraph:

In step 422, the change made by the administrator is reflected in the policy server database 130. In this regard, branches 264 and 266 of the LDAP tree are modified accordingly to reflect the change in the policy setting. Additionally, in step 424, the policy server 122 creates a log of the changes for the administrator for later processing and sending to the appropriate policy agent. In step 426, the policy server 122 updates the administrator's log DN 270d to reflect the change. In the above example and as illustrated in FIG. 24, if the log created is named "A_L1," the policy server 122 updates the DN 270d for "adm" at "domain1" to create an attribute "apply" 270f that has the value "A Li" 270g. Other changes made by the administrator are reflected in separate logs (e.g. "A_L2," "A_L3") and appended to the existing value of the apply attribute in the administrator's log DN 270d.

Please replace the first full paragraph, of page 41 with the following amended paragraph:

The changes suitably modified for each policy enforcer's LDAP are then stored in a device log. Each policy enforcer's log DN 270e is then modified to reflect the change to the transmitted ~~to the~~ particular policy enforcer. In the above example and as illustrated in FIG. 24, if the device log created is named "PE_L1," the policy server 122 updates the DN 270e for the particular policy enforcer "PE1" at "domain1" to create an attribute "apply" 270i that has the value "PE_L1" 270j.

Please replace the second full paragraph, of page 43 with the following amended paragraph:

The primary unit 902 responds to the "Keep Alive" packet by changing the command field of the packet to a KEEP_ALIVE_RESP command and re-transmitting the packet to the

sender. If the backup unit 904 does not receive a response back from the primary unit 902 for a predetermined period of time (e.g. one second) for one "Keep Alive" packet, the backup unit 904 begins preparing to take over the active role. Preferably, the predetermined period should not be greater ~~less~~ than two consecutive "Keep Alive" packets.

Please replace the fourth full paragraph, of page 45 with the following amended paragraph:

In step 956, the primary unit is checked to determine whether it is functional. If it is, the primary unit is likewise updated 962 with the configuration change. Otherwise, if the primary unit is not functional, the backup unit takes on the active role and becomes the active unit in step 958. The primary unit may become non-functional and thus, inactive, due failures in the CPU board, the network interface card, or power supply.

Please replace the third full paragraph, of page 46 with the following amended paragraph:

FIG. 30 is an exemplary flow diagram of updating the primary and backup units when the primary unit is not functional. In step 978, the primary unit becomes nonfunctional, and in step 980, the network administrator sends/transmits an ~~upgrade~~ update directly to the backup unit instead of the primary unit. In step 982, the backup unit updates itself with the information received from the management station and waits for the primary unit to become functional 984. Once the primary unit becomes functional 984, the update is automatically sent/transmitted to the primary unit for upgrading in step 986. The primary unit then updates itself in step 988.

Please replace the Abstract, on page 52 with the following amended paragraph:

ABSTRACT OF THE DISCLOSURE

A unified policy management system for an organization including a central policy server and remotely situated policy enforcers. A central database and policy enforcer databases storing policy settings are configured as LDAP databases adhering to a hierarchical object oriented structure. Such structure allows the policy settings to be defined in an intuitive and extensible fashion. Changes in the policy settings made at the central policy server are automatically transferred to the policy enforcers for updating their respective databases. Each policy enforcer collects and transmits health and status information in a predefined log format and transmits it to the policy server for efficient monitoring by the policy server. For further efficiencies, the policy enforcement functionalities of the policy enforcers are effectively partitioned so as to be readily implemented in hardware. The system also provides for dynamically routed VPNs where VPN membership lists are automatically created and shared with the member policy enforcers. Updates to such membership lists are also automatically transferred to remote VPN clients. The system further provides for fine grain access control of the traffic in the VPN by allowing definition of firewall rules within the VPN. In addition, policy server and policy enforcers may be configured for high availability by maintaining a backup unit in addition to a primary unit. The backup unit ~~become~~ becomes active upon failure of the primary unit.

## Amendments to the Drawings:

The attached sheets of drawings include corrections to Figs. 2 and 26 as follows: In Fig. 2 reference number 226 referring to the admin policy is being corrected to reference number 228 as it is referenced in the text. In Fig. 30, the reference numbers 445, 450 460, 465, 470, and 480 are being omitted as extra reference number that do not pertain to anything with regards to the invention.

Attachment: Replacement Sheet for Figs. 2 and 30
Annotated Sheets Showing Changes to Figs. 2 and 30 as originally filed.